

CONSUMER PROTECTION COMMITTEE

of the

SUFFOLK COUNTY LEGISLATURE

-

Minutes

A regular meeting of the Consumer Protection Committee of the Suffolk County Legislature was held in the Rose Y. Caracappa Legislative Auditorium of the William H. Rogers Legislature Building, Veterans Memorial Highway, Smithtown, New York, on Wednesday, **March 9, 2005**.

MEMBERS PRESENT:

Legislator Cameron Alden • Chairman

Legislator Jay Schneiderman • Vice•Chair

Legislator Lynne Nowick

Legislator William Lindsay

MEMBER NOT PRESENT:

Legislator Jon Cooper

-

ALSO PRESENT:

Mea Knapp • Counsel to the Legislature

Warren Greene • Aide to Legislator Alden

Charles Gardner • Director of Consumer Affairs

Ilona Julius • Deputy Clerk of the Legislature

Kevin Rooney • Oil Heat Institute

Peter Grupe • Special agent • Federal Bureau of Investigation

Michelle Di Benedetto • Director of Government Relations • Citibank

John Cowie • Suffolk County Police Department • Computer Crimes Unit

Tom Gabriele • Suffolk County Police Department • Computer Crimes Unit

Jim Crayne • Suffolk County Police Department • Computer Crimes Unit

-

MINUTES TAKEN BY:

Donna Catalano • Court Stenographer

(* THE MEETING WAS CALLED TO ORDER AT 1:10 P.M. *)

CHAIRMAN ALDEN:

Good afternoon. And welcome to the Consumer Protection Committee. We're going to start with the Pledge, and we'll have Legislator Schneiderman lead us in the Pledge.

LEG. SCHNEIDERMAN:

All rise, please.

SALUTATION

CHAIRMAN ALDEN:

I usually ask for a moment of silence in honor of those troops who have actually paid the supreme price for us. We still have troops all over the world who are fighting even as we speak right now. So I just ask for a quick moment of silence.

MOMENT OF SILENCE

CHAIRMAN ALDEN:

Thank you. We actually don't have a long agenda as far as things to vote on, but we have some very important business to take care of today. We're going to look at a little bit of this problem with identity theft. But first we have one card for the public portion, and that's Kevin Rooney. Hi, Kevin.

MR. ROONEY:

For the record, my name is Kevin Rooney. I'm the Chief Executive Officer of the Oil heat

Institute of Long Island. I would like to offer a few brief comments in support of Introductory Resolution 1037•2005, which is a tabled resolution later in the agenda.

This proposal would require the installation of carbon monoxide detectors in residential dwellings on the occasion of the replacement of an existing fossil fuel heating system. Under less than optimal operating conditions, all fossil fueled heating systems are capable of producing carbon monoxide, albeit at different stages of the combustion cycle. The installation adjacent to sleeping areas of a plug•in CO detector with backup battery provides a simple cost effective warning device to homeowners of unacceptable levels of carbon monoxide. The installation of carbon monoxide detectors is strongly recommended, not only by the Federal Consumer Product Safety Commission, but also by the oil, gas and propane industries.

The homeowner and installer certification procedures, which we understand are now part of this resolution, will furthermore allow the Office of Consumer Affairs to monitor compliance with the new law on a County•wide basis. And we would like to commend the prime sponsor, Legislator Caracciolo, for making those changes and thus making the law more effective.

If one single life is lost due to the lack of an operating carbon monoxide detector, then that was one life too many. This legislation will not only protect the health and safety of County residents, it will also save lives. And on that basis alone, we strongly urge your support of resolution and its expeditious enactment. Thank you very much, and I will gladly answer any questions.

CHAIRMAN ALDEN:

Legislator Nowick.

LEG. NOWICK:

Thank you for your presentation. And I just have a question, maybe more on a personal learning

level, did you say that those portable plug-in units are supposed to be plugged in by the bedroom?

MR. ROONEY:

The recommendation from the CPSE, Consumer Product Safety Commission, is that carbon monoxide detectors be located adjacent to sleeping areas.

LEG. NOWICK:

Is that so you can hear it? Because that would mean it has to go from the basement, go all the way •• particularly, I'm thinking of my own home •• it has to go from the first floor, then up to the second floor?

MR. ROONEY:

When individuals, adults, children, seniors, are sleeping are those periods most when they are most vulnerable to carbon monoxide inhalation, and therefore •• and therefore, health and safety problems related to that. If you are awake, for example •• if you are awake, the symptoms would be similar to a mild flu, headaches, nausea, possibly respiratory problems in seniors, all of which are indicative of carbon monoxide poisoning. When an individual is asleep, obviously, then they are most vulnerable to not physically experiencing those symptoms that would •• that are, in essence, the early warning stages of CO poisoning.

LEG. NOWICK:

Okay. And I'm just thinking in terms of safety in my own household, I put one downstairs and I put one on the second floor.

MR. ROONEY:

I don't •• I'm not saying you shouldn't.

LEG. NOWICK:

I'm just trying to learn.

MR. ROONEY:

If a homeowner installs one, that's where it should be. Should there be one on the lower floor?
If they want to go to the expense of doing that, yes, absolutely.

LEG. NOWICK:

But near the bedroom so you can hear it, I guess.

MR. ROONEY:

Right. That's exactly the case.

LEG. NOWICK:

Thank you. I just needed to learn that.

CHAIRMAN ALDEN:

Legislator Schneiderman.

LEG. SCHNEIDERMAN:

I just have the amended copy of the bill, and I'm trying to look through it, but maybe you can answer some basis questions. The title of the bill deals with conversion. Would the homeowner have to switch from one type of heat to another for this to be triggered?

MR. ROONEY:

No. It's actually by conversion. You are thinking from converting from one fuel to another. No. This is really upon the installation of a replacement heating system. It could be from oil to oil, gas to gas, oil to gas or gas to oil.

LEG. SCHNEIDERMAN:

And is there currently a requirement that a carbon monoxide filter be installed in a new home at the time •• the first installation?

MR. ROONEY:

Yes, there is.

LEG. SCHNEIDERMAN:

There is. Okay. So this would capture ••

MR. ROONEY:

On all new construction, CO detectors are required as approved by Suffolk County Department of Health Services a number of years ago, and those are hardwired with battery backup.

LEG. SCHNEIDERMAN:

Typically, in a new home, when you're putting the heating system in, you put your carbon monoxide filter in, you are not going to get a CO from your local building inspector until you demonstrated that you have an operating CO detector. How are we going to know if people are complying with this law? What is the mechanism?

MR. ROONEY:

One of the changes that was passed by myself and Consumer Affairs was a simple certification procedure, whereby the installer, be it a heating oil company, a gas subcontractor, a HVAC or plumbing company, would provide this certification to the •• to the homeowner. That certification would be filled out at the time of the replacement unit, and that certification would then be sent to the Department of Consumer Affairs. And the forms would be generated by Consumer Affairs and maintained by them.

LEG. SCHNEIDERMAN:

I suppose that could work. It's not as fail•safe as the •• you know, we don't have an inspector in

the house after that. You don't need to get a permit, I don't believe, to convert your heating system, do you?

MR. ROONEY:

Many towns require a permit for the installation of any heating system, but it does not require an inspection.

LEG. SCHNEIDERMAN:

Okay. But you would need a permit just to •• let's say you got a gas burner and you want to swap it out with a new gas burner, you wouldn't need a permit for that?

MR. ROONEY:

Some towns require a permit.

LEG. SCHNEIDERMAN:

Some towns do. So in those towns, they can enforce this at that point.

MR. ROONEY:

Possibly.

LEG. SCHNEIDERMAN:

If the building inspectors are aware of it?

MR. ROONEY:

Possibly. But the enforcement then becomes very diffused as to whether or not permits are being issued by some towns and not by others, for what kind of work, whether their village permits, town permits. Realistically, having the County Office of Consumer Affairs monitor this through a certification process is far more effective in our opinion.

LEG. SCHNEIDERMAN:

It wouldn't be triggered by modifying your heating system, right? Let's say you were taking you oil tank out of the ground, which is something we've been trying to encourage through incentives
••

MR. ROONEY:

We agree.

LEG. SCHNEIDERMAN:

•• and putting it in •• I know that you do. And putting it above ground, that would not trigger this requirement?

MR. ROONEY:

No.

LEG. SCHNEIDERMAN:

Only ••

MR. ROONEY:

No. It has nothing to do with the heating system per se.

LEG. SCHNEIDERMAN:

Okay. So it's not modification to heating systems, it's a completely •• it's a brand new heating system?

MR. ROONEY:

That is correct.

LEG. SCHNEIDERMAN:

What are the costs? What's the financial impact to the homeowner? What does it cost for one of these carbon monoxide detectors?

MR. ROONEY:

They run •• correct me if I'm wrong here, Charlie. They run anywhere from \$70 for a rather basic model up to about 120 to 150 for a very sophisticated model. My daughter who happens to, God forbid, live in a gas heated home ••

LEG. SCHNEIDERMAN:

I thought you were going to tell me she owns the company.

MR. ROONEY:

She bought the house with it. Anyway, she actually has three plug•in CO detectors in her house, because the basement is partly above ground. The units that she put in, I brought them at Home Depot outside of Morristown, and they were like 120 a piece.

LEG. SCHNEIDERMAN:

One hundred twenty is the approximate cost of compliance. You only have to put one in?

MR. ROONEY:

That is correct. It's a minimal cost for potentially maximum savings if you consider life to be the maximum saving.

LEG. SCHNEIDERMAN:

More than a smoke detector?

MR. ROONEY:

Oh, yeah, way more than a smoke detector. You can buy a smoke detector at Home Depot for 15 bucks.

CHAIRMAN ALDEN:

Legislator Nowick.

LEG. NOWICK:

Did I understand that this bill would require the CO detectors to be put on the furnace itself?

MR. ROONEY:

No. God no. No. That's the last place in the world. Otherwise that thing would go off all of time. No. This would be •• it is a unit that is simply, you know, plugged in in a hallway adjacent to bedrooms.

LEG. NOWICK:

Can I just tell you a quick •• we have a minute, so I'll just tell you a quick story, my experience, and I have two of these units. I did hear it in the middle of the night go off about a month and a half ago. I heard that strange noise, which •• I guess I was on the ladder up at the smoke detector taking every one of my smoke detector batteries out because I couldn't figure out what

it was. But it was the unit downstairs, the CO detector. You know what? And I thought to myself is this working. Not to take any chances, I did call 911, and just so you know about it, our Police Department was there within seconds. They made me get out of the house. Just to make a long story short, the fire department, one showed up at 4:30 in the morning, the Police Department with the lights, the fire department with the lights, fire department vehicle with the lights. Four thirty in the morning, the hook and ladder pulls down my street with the lights and then another vehicle. Out of the hook and ladder come three men with the Ghostbusters thing on the back, went in the house, not a neighbor woke up, nobody woke up, nobody. But they said that the most important was that I called. And it was okay. It was a faulty detector.

LEG. COOPER:

Have you subsequently disconnected all of your CO detectors?

LEG. NOWICK:

I called the company. Rather than buying new ones, I called the company, they immediately sent out two more. After that, my smoke detector started, beep, beep, beep. But, you know, it's very important they told me. They told me get out of the house immediately. So be careful to monitor those that they're not faulty.

MR. ROONEY:

Mr. Cooper, her ability to withstand embarrassing moments went up enormously.

CHAIRMAN ALDEN:

I'm glad that this emergency happened in Smithtown where there's plenty of the police coverage in the midnight to eight hours.

MR. ROONEY:

I don't want to go there.

MR. ZWIRN:

Seconds. They were there in seconds, Cameron.

MR. ROONEY:

Are there any other questions, Mr. Chairman?

CHAIRMAN ALDEN:

Kevin, quick touch on this. We got hit with a cold spell now, and how are we looking as far as oil reserves and things like that? Looking real bad?

MR. ROONEY:

Can I plead the Fifth?

CHAIRMAN ALDEN:

We can look for a big spike, right?

MR. ROONEY:

Since you got me, given the fact that crude oil is now up around •• I checked it back at the office •• fifty•five twenty•eight on the April contract, that is the Mercantile Exchange Futures Market. Realistically, the problem that we have in my industry now is that to all intents and purposes, the refineries are looking at this heating system •• heating season as pretty much over. They begin turning over their inventory starting around about the second or third week of February, and they start producing less quantities of distillate products, ie, heating oil and diesel fuel and start producing larger quantities of gasoline in order to build up supplies for the season. So when you have exceptionally cold weather that hits in March and even April, what that means is there's not enough output of heating oil and other distillate products at the refineries, we end up having to import it.

We are now probably importing about two to three times the normal level of heating oil from Europe. And the product heating •• distillate product coming off Rotterdam Spot Market is running at about anywhere from eighteen to twenty cents a gallon higher than domestic product from the domestic refineries. So we've got a two or three week period here where we're looking at the potential for extreme volatility in wholesale heating oil prices before they really begin slacking off.

So, you know, the only thing I can say is, you know, unless someone is actually going to get a delivery in the next couple of few weeks, most people will be largely unaffected by it. But that's •• that's what's essentially going on right now, it's a higher level of imports.

CHAIRMAN ALDEN:

Thanks a lot.

MR. ROONEY:

You're more than welcome, sir. Thank you.

CHAIRMAN ALDEN:

I invited FBI Special Agent Peter Grupe to talk to us today about identity theft. So at this point, I'm going to call him up. And Ben Zwirn, actually this is a good catch on Ben's part, saw that I had that on the agenda and decided to invite the County guys that actually do some work in this regard too. So I'm going to thank Ben for that. We also have with us Detective Sergeant John Cowie, Detective Tom Gabriele and Detective Jim Crayne, and I would invite them up too. I think we should have room for everybody up here. Michelle is going to come up too, Michelle Di Benedetto is Citibank's Director of Government/Community Relationships, and they've actually developed a program to try to help some of the community and other people that might be affected, some of their customers, with identity theft. So, Pete, I guess we'll start with you. I was fortunate enough to go to a Chamber of Commerce Meeting where the Special FBI Agent made a presentation, I think it was very, very valuable. That's why I asked him to come and address us today. And hopefully, out of some of these meetings, we can maybe get a good handle on what's going on out there. And maybe there might be some things that Suffolk County can do to make people aware of steps that they can take to either mitigate the damages or prevent identity theft. So thanks a lot for coming down today.

MR. GRUPE:

Thank you, again, for having me here today. It's a pleasure to be here. I'm here to discuss a very serious problem, identity theft. A problem that's confronting certainly citizens of this country and the County of Suffolk. My name is Peter Grupe, I'm a Supervisory Special Agent with the FBI here in Melville. I'm responsible for all white color crime investigations on Long Island.

I just wanted to get started and read a press release dated January 11, 2005, from United States Attorney for the Southern District of New York. The title of the article is, "United States Announces Sentencing of Man in Largest Identity Theft Case in Nation's History". United States Attorney David Kelly for the Southern District of New York announced that Philip Cummings was

sentenced to 14 years in prison in Manhattan Federal Court today for his role in a massive scheme to steal the identities of up to 30,000 people. He was ordered to forfeit a million dollars in proceeds. Cummings had worked for a company as a help•desk employee, a technology company that provided his customers with computerized access to the three commercial credit history bureaus. He had access to confidential passwords, subscriber codes pertaining to customers who used the software to download credit histories.

Together with a coconspirator, they accessed credit bureaus and downloaded more than 30,000 consumer credit histories from about early 2002 through October of 2002. The reason I start this and bring this to everybody's attention is where is this company located? Bay Shore, New York, okay. As of January 11, 2005, this was the largest identity theft case in the country, all right, in the nation's history. So obviously, we can't get much closer than that. It's a problem in Suffolk County as well as all over the country.

If I can just take a step back and just talk a little bit about the FBI and some of the things that the FBI does. The FBI is located in Melville. We have approximately 50 Special Agents assigned to the New York Office in Melville. We've got another thousand agents assigned to the Manhattan Office, Queens, White Plains and so forth. The FBI is responsible for investigating over 300 violations of federal law; everything from terrorism, civil rights, organized crime, white collar crime, foreign counterintelligence. We've got a lot to do. And the reason I bring this to everybody's attention is really the key to this is awareness and prevention.

I'll be very busy with or without identity theft, with or without cases coming across my desk everyday. The key is to prevent it before it does become a crime, and I think that burden is upon the consumers and some of the financial companies that we deal with each and every day. What is identity theft? If you have been charged for a purchase you didn't make, received a bill for a credit card you did not open, received a product you didn't order, find that your credit report includes debts you never knew you had, discovered funds missing from your account, you're a victim of identity theft. Identity theft simply means that someone is using identification

without your permission.

Possible outcomes as a result of that; credit history with negative information, a criminal record even though you've never been arrested, you've receive bills for purchases you never made, outstanding loans for which you never signed for. What that all adds up to you as the consumer or a victim is significant expenses, times and headaches in attempting to clear all this up.

Legislation now states that the consumer, the victim, if you were defrauded, if you report the theft to the financial institution, credit bureaus, within two or three days, your total liability would only be about \$50. If you wait 30 days, I think it could be \$500. So the key is to stay on top of your accounts, your financial activity and try to become aware of that as soon as possible.

In 2004, approximately 9.3 million people were victims of identity theft. Over 33 million people have been victims of identity theft since 1999. Businesses will loss approximately \$4.2 million this year alone •• excuse me, \$4.2 billion, that's with a B, 4.2 billion this year alone. And they expect that number to grow to about eight billion by 2006. This is a serious problem. The financial victims, again, ultimately are the credit card companies, banks, and other financial institutions. You as the consumer will suffer, as I described before, by trying to clear up this mess.

We've had individuals arrested. People becoming aware of criminal histories that they have as a result of somebody stealing their identify, committing a crime and being arrested. I've had people come to me and say, I have a criminal history I didn't even know I had. We had an individual who was arrested in San Diego, California, using your identification. So this can go from a very minimal \$100 charge on your credit card to perhaps a criminal history in your name. There's a wide diverse expanse of potential problems.

Recent article, a Delaware couple are accused of misusing personal information for more than 30 hospital patients resulting in obtaining credit cards and checks in someone else's name. Again, this is the ability •• or the capability of somebody getting your information. Recent articles within the last two weeks were a result of the intrusion into a credit reporting system called Choice Point. Choice Point is a service that's used by law enforcement agencies, private investigators, so on and so forth, that contains a ton of information about you and millions and millions of people in the country. What happened was somebody had infiltrated the Choice Point system in California, and they were able to steal many, many information •• much information from individuals.

Recent newspaper article, "Are You Next?" Thousands of New Yorkers are about to learn their identities have been stolen. Nine thousand three hundred and seventy New Yorkers will get the very bad news that their identities were stolen; personal information from Social Security account numbers, credit histories, etcetera, are in the hands of criminals. And that's the Choice Point case that I was just referring to. That's caused Senator Schumer and many others to really take a look at identity theft and the growing epidemic that we have.

Earlier this year, Visa, Mastercard and American Express confirmed that a hacker had accessed eight million credit card records from those accounts. "Identity theft is for the information age what bank robberies were to the depression era," Senator Charles Schumer. How do identity thieves get your personal information? They steal wallets and purses containing your identify, identification, credit, bank cards and Social Security. They'll number steal your mail, they'll complete a change of address form and divert your mail to another location. They'll rummage through your trash, also called dumpster diving. Think of all the personal information you throw out every day that if it gets in the hands of the wrong individuals, it can be very, very problematic.

They'll fraudulently obtain your credit report. That's kind of what I was referring to before in

some of the other newspaper articles. They find personal information in your home. They scam you through e•mail. There's a very popular problem nowadays. It's called phishing, p•h•i•s•h•i•n•g. Again, many, many articles recently about phishing. And what that is is the use of the internet or e•mail to get information from you. What will happen is they will send you an e•mail requesting some information, they'll have you click on a website, this website has been designed, adapted by criminals and that allows them to get more information from you. The use of the e•mail can simply be just giving them dates of birth, Social Security account numbers to let them go. Phishing just a little bit more complicated than ordinarily just getting information this information from you online. But it's a very, very hot topic and something that everybody should be aware of.

They get information from the work place in a practice known as business record theft. They get your information through other repositories like hospitals, doctors' offices. Think about all the information that your doctor or your dentist or somebody has every time you walk in to your doctor's office. You're greeted by a receptionist. Well, behind a receptionist are thousands and thousands of files. These files contain information which would allow the bad guys or thieves to perpetrate a crime against you. All they really need, the basic information they need, is your full name, date of birth, Social Security number. Those three items that allow them to perpetrate many, many frauds against your name. They've stolen your identity, they're opening up credit cards, bank accounts, which you are not even aware of. An ID thief just simply needs that information to open up credit and bank accounts.

Some examples of cases that FBI and law enforcement have been involved in recently. A major Wall Street firm had many employees that were victimized through identity theft. I had received a lead from our office in Charlotte, North Carolina. A bank had been •• some banks had been some photographs were provided to me dealing with counterfeit checks and opening fraudulent bank accounts. Some of the people and the credit card holders that had been victimized worked for this wall Street firm. I went down, I interviewed some of the victims down there in Lower Manhattan. I showed this grainy black bank surveillance photograph to these individuals, they all pointed him out, they identified him. He was a custodian who worked the midnight to eight shift. Every night all he did was walk around the office looking at information that the employees

had left on their desk or just in open desk draws not locked. My point here is to safeguard all your private and personal information. People have access to your information just simply by going through your mailbox, going through your place of employment. These are all opportunity to steal your identity.

Nigerian letters and e-mails, okay. We've all •• I think Mr. Alden sent me some letters that were received recently. These are attempts made by individuals, they originated from Nigeria way back when they were sending out mass mailings. Basically in some and substance, what it was is they have money, they've got money in Nigeria, they've got money in South Africa which they want to get out of the country. They need a repository in the United States, they need a bank account to deposit that money. They'll go off on various tangents as to why they need to do this in a secretive fashion. What they need is a bank account to deposit the money. What will they give you? They're going to give you twenty five to 40% of \$17 million. It's always a huge substantial amount of money. If they send out 5000 of these mailings and four or five people bite, they're way ahead of the game, all right? What they do then is they have your bank account information, some people even divulge Social Security account numbers, dates of birth and everything, I've seen a wide variety of people being victimized as a result.

These are •• the mass mailings have been replaced by mass e-mails. They send out e-mails. If anybody's on their e-mail each and every day, over the last couple of years, you probably have been recipients of one of these e-mails. Again, it's a numbers game. If they send out 5000 and get three or four, they're very, very happy. This results in credit card accounts, bank accounts being opened in your name and you being victimized.

Stories and examples go on and on. I could tell you many, many stories. We had a situation shortly after 9/11, '01. We had a lead, a terrorism lead where we had individuals in Staten Island who neighbors called and thought they may be involved. I went out there, looked at the address, did a couple of things. These are people involved in white color crime, we ruled out terrorism. Sitting outside of the house, I ran the license plate on the car. This car was stolen.

It was a rental car down in Virginia, it was never returned. It was rented about three or four months ago. So now I'm getting more and more interested. Long story short, the person whose name the car was rented under was a retired New York City Police Officer. I contacted the New York City Police Officer, he said, "Pete, I'm glad somebody finally called me." He said, "I cringe everyday the mailman walks up my driveway." Why is that? I'm getting bills for purchases I never made, credit cards I never opened, rental cars I never rented. It went on and on and on. Long story short, I was able to track it back. He purchased some jewelry in a jewelry store in Bay Ridge, Brooklyn. They were able to get his credit card information and some other personal information from him when he purchased his jewelry. The people who lived in this house in Staten Island, the sister worked in a jewelry store, provided them with this information. This is just one of many examples of how this can happen.

How can identity theft be prevented? Carry only those cards you actually need. Don't carry your Social Security card. Everybody in this room knows what their Social Security Account Number is, why do we carry our Social Security card, okay? These are things that can be misplaced, viewed by others, and obviously, you become the victim. Review your accounts regularly. One of advantages of the internet is the ability is to track and monitor your accounts on a daily basis. All right. If you become a victim today, if you look at your e-mail and track banking online, perhaps two or three days from now, you're going to see a discrepancy, a red flag is going to go up, you're going to notify your bank. If you review your accounts once a month when you receive your bank statement, in thirty days the losses may be \$30,000 as opposed to maybe two or \$300, all right? So the key is to review your statements on a regular basis. Online banking, the internet allows you to do that.

Don't put your red flag up on the mailbox. A red flag is exactly that, a red flag for the bad guys to know you have mail in your mailbox. Think about all of the things you put in your mailbox to be sent out that contain your checks and other personal information. The mailman is going to stop at your house whether you have that red flag up or not. Don't literally throw up a red flag. Somebody comes by, takes the mail that hasn't been mailed yet, they're able to get copies of your checks, produce counterfeit checks. These are all examples of cases that I've seen and victims •• how individuals have been victimized.

Safeguard all your passwords and your PINs. Don't use obvious ones like your sons' names, your daughters' names, date of birth, things like that. Keep personal items in a safe place at home. Think about some of the people we allow into our house, whether it's carpet cleaning services, people that come that are virtual strangers. They come into your house, within a span of 15 to 20 minutes, you are in the kitchen, they're in your bedroom. Okay. They see a checkbook. What they're going to do is they're not going to steal a check that's sitting right on top, they're going to steal a check that at the bottom of the checkbook. All right. They're going to steal the last check, all right? Why? Because it's going to be perhaps a couple of weeks before you realize that it's missing. At that point, they've written a check against your account, and the money's gone. These are just little things. Keep all your personal items in a safe secure place at home. We think we're secure at home, we're not always that secure. We have repairmen, contractors, people like that coming through your house on a regular basis.

Obtain a copy of your credit report on a regular basis, at least every six months, at the very least, once a year, just to identify what accounts you have there to notice any discrepancies, any accounts you are not aware of you. The computer has become so popular, the internet has become so popular. Go out and spend \$49 for a computer software to have a fire wall, a spy software installed on your computer. This will go a long way to avoid people hacking into your computer system or allowing some of these phishing•type crimes to occur.

There's also a load of services that you can use for \$9 a month which will monitor your accounts for you. These have become very popular as a result of what I've been describing for the last few minutes. And then very simply, buy a shredder for all your documents. Just because you put it in a bag, you wrap the bag up, put it out by the curb, it doesn't mean it's secure, okay? Spend the extra few minutes. Buy a shredder, shred your documents. Again, I can go on and on about this topic, it's very, very diverse. It can be a very complicated topic, but it is something that each and every one of us should be aware of. It's not going to get better, it's going to get worse before it gets better. Thank you.

CHAIRMAN ALDEN:

Legislator Cooper indicated that he had some questions or comments.

LEG. COOPER:

Just one. Peter, you had suggested that one of the things the people can do prevent identity theft was to not carry their Social Security Card with them, and I don't carry my Social Security Card, but I know that every member of this committee carries a card that lists our Social Security Number, and it's our health insurance card. They use your Social Security Number as the ID number. This is VYTRA. I also have Blue Cross, they use my Social as their ID number.

CHAIRMAN ALDEN:

Can I see that number for a minute, Jon?

LEG. COOPER:

If you show me yours. Has legislation been proposed, do you know, that would prohibit health insurance companies from using Social security numbers as ID numbers? They could come up very easily with their own IDs.

MR. GRUPE:

Not that I'm aware of. But I think you're going to be seeing more and more of that proposed legislation in the next year or so.

LEG. LINDSAY:

We could change the County process. Why don't we direct VYTRA not to use it?

CHAIRMAN ALDEN:

Jon told me he was handling that, so I just took, you know, like, a back seat to it.

MR. GRUPE:

A lot of the examples you •• there are a lot of examples of what you are describing, that people over the last several many years looked at it very innocently. But as a result of what's transpired over the last few years, people are looking at it in a different light and making suggestions, recommendations just like you are or like I had been for the last few minutes to include, you know, let's not use Social Security Account Number as identifiers for health insurance and other things. Senator Schumer, other Legislators like yourself, are doing just that, looking for ways to prevent these types of occurrences.

LEG. COOPER:

Thank you.

CHAIRMAN ALDEN:

Legislator Nowick.

LEG. NOWICK:

Two questions. The term phishing. I'm not sure that I know •• I would recognize it if I saw it come across the internet, and yet somebody did question me not too long ago about these e-mails that come through, you've won \$250 free Home Depot money, then they go into 200 questions that you have to answer. Could that be a phishing thing or that up and up type of thing?

MR. GRUPE:

That can be a phishing thing. The problem is there are many, many legitimate requests and then •• but there are many that are not legitimate. Something that you just described, yes, could be a form of phishing. Let me see if I can give you a better •• all right. Phishing, an internet fraud that is surging into e•mail boxes with a vengeance. By sending phony e•mails to thousands of electronic mailboxes, cybercrooks hope to lure you to a fraudulent or spoofed website where you'll be tricked into divulging personal information. Typically what happens is you receive an e•mail requesting information. Phishing •• I think you might be able to go into a little more detail with this •• but what they're looking to have you do is to click a website that has been set up by the bad guys which will allow them to get further information from you. It can include the very straight forward example you used or something that's far more intricate or complex.

LEG. NOWICK:

All right. And the other question I had for you is I've always worry about shopping on the internet, yet I would book airline flights through Southwest because it's a pretty much •• any time you go to eBay, you're always giving your credit card and your expiration number and the three digits on the back. Is that secure?

MR. GRUPE:

A very controversial topic these days is because of the increase in technology, the increased use of e•mail, you know, are we really allowing these to be perpetrated? Is identity theft only a problem because of the technology and the increase in popularity of the internet? If you spoke to 100 people, you'd get 50 yeses and 50 nos. Identity theft existed long before the internet and e•mail became popular, all right? But recently, with examples like Choice Point, the company in Bay Shore, it's made it easier, because websites, data bases have become repositories for all this information.

LEG. NOWICK:

Can they get into the sites, like a Southwest site, or eBay, or when you go shopping •• you can go shopping on the internet, you can go to Penny's, Macy's, and you do wind up giving your credit card number, you have to. Can these hackers get into these sites also?

MR. GRUPE:

I think the reality of it is, again, depending upon the level of sophistication, if you have a sophisticated hacker •• I'm trying to think of the example, it was about two months ago, Verizon that was •• it was a major corporation, their computer system was hacked into. We have had US government data bases hacked into. What happened is these companies now are spending more and more money to encrypt the information, to set up firewalls to prevent this. The answer to your question is yes. You know, again, it depends upon how much money, how many much •• how much resources these companies have spent to prevent being hacked into, all right? Choice Point, again, the example I used at the outset, has a wealth of information on everyone from the President of the United States all the way down to John Q. Citizen. Choice Point was infiltrated, and that's why Senator Schumer and many others are really taking a look at legislation to prevent this, Whether it's requiring banks and financial industries to have encrypted software, to have firewalls installed. Right now, it's kind of a very loose requirement. They're looking to pass legislation to require Southwest Airlines to have a certain level of encryption to prevent their data base from being hacked into.

LEG. NOWICK:

It certainly does become frightening, doesn't it?

MR. GRUPE:

It does. But, you know, I think the advantages of the technology and the internet far outweigh the potential problems, but it does create opportunities for thieves.

LEG. NOWICK:

Last question. Still have Frank Anagnale working for you guys?

MR. GRUPE:

Yes. Yes, we do.

LEG. NOWICK:

He teaches a lot of good things.

MR. GRUPE:

I spent about three days with him in New Orleans last year.

LEG. NOWICK:

He is incredible.

MR. GRUPE:

He is a brilliant, brilliant man.

LEG. NOWICK:

Incredible.

MR. GRUPE:

And what he is doing now •• have you met him?

LEG. NOWICK:

Several times I've heard him speak.

MR. GRUPE:

He's terrific.

LEG. NOWICK:

And you are glued to him when he speaks.

MR. GRUPE:

He is making millions now, legitimately, by •• as a consultant. His firm is a consultant to financial industries, banks, brokerage firms. And he tells them how to prevent being victimized and being defrauded. Who better to tell than Frank Abagnale. What he is doing is exactly what we just described, hey, Southwest Airlines, this is what you need to do, hey, you know, Bank of America, this is what you need to do. Everything from these are the types of checks you should be producing to these are the types of computer systems you should be utilizing. It's exactly what he and others are doing now very successfully.

LEG. NOWICK:

I think it's wonderful. For those of you who don't realize he was •• well, Catch Me If You Can, right.

MR. GRUPE:

Yeah.

LEG. NOWICK:

Thank you. Thank you very much, very, very informative.

CHAIRMAN ALDEN:

Legislator Schneiderman.

LEG. SCHNEIDERMAN:

Thank you, all of you, for coming out today to talk to us. It is •• it's a very real issue. I know people think it will never happen to them. A couple of quick stories. My mother•in•law recently wrote a check for someone, you know, I think it was, like, I won't say the establishment, but somebody then took the check, I guess, photocopied it and reproduced artificial checks, and took one to a bank teller and tried to cash a \$3000 check. Another example •• and this really, I think, demonstrates the vulnerability of senior citizens to identity theft, but my father who is 83, a couple things started to happen, one is somebody had gone to a local pharmacist, and probably with a phony prescription as well for drugs with a note, with his name forged saying that this other individual could charge on his credit card. And fortunately, we were able to catch that person who did that, but not before they were able to obtain a significant amount of drugs, which who knows whether they sold those drugs or abused those drugs. But it really struck close to home, because these things really do happen, as you illustrated in you first example with the largest case being right here in Suffolk County. You mentioned that you thought it was a good measure to check our credit reports, so, first, tell us, how do you do that? That's my first question.

CHAIRMAN ALDEN:

Michelle actually might be better, because she's from the banking industry.

LEG. SCHNEIDERMAN:

Okay. We can come back to that. I know they've made it easy and free to do that. And I think it's good just as a public service•type announcement to alert the public as to how to check their own credit reports.

LEG. NOWICK:

On that point, if I might interrupt, I know Bank One was giving you a thirty day free trial as part of their service. I think Bank One took over some of the Visa Cards. And you were able to get your credit report for the first month, and then if you stay, for \$11 a month, you can continue to get it.

CHAIRMAN ALDEN:

It's not a paid endorsement, is it?

LEG. NOWICK:

No, but you know what? I got the free report.

LEG. SCHNEIDERMAN:

Well, we'll get more information on that in a second.

MR. GRUPE:

You can just simply contact the three major credit bureaus. They are Equifax, Experian and TransUnion.

LEG. SCHNEIDERMAN:

Okay.

MR. GRUPE:

And they'll give you your credit report.

LEG. SCHNEIDERMAN:

There's two other vulnerabilities that I don't think you mentioned, maybe you did, very often, you know, you go out to a restaurant, wherever it might be, you pay by credit card, and you get your credit card receipt, and many of those receipts have your credit card straight across. So it's not your Social Security number, but your credit card number, which is certainly vulnerable to being abused. You know, I think oftentimes, we throw those out in the garbage. I think people really need to be careful. It used to be the carbon copies that people would use, they would have your signature on them.

MR. GRUPE:

That's a problem. Again, I was trying to address kind of the technological advances and some of the large scale Choice Point-type problems that we've encountered through phishing or other means. But that's kind of like •• that's all reliable, that's something that's been going on for many, many years, somebody •• the waiter or the waitress in the restaurant stealing your credit card and getting your credit card number.

LEG. SCHNEIDERMAN:

Right. We had a situation, somebody who was working at a resort was taking those credit cards and then mail ordering stuff to summer homes that nobody would be around in the winter, and then picking them •• they caught him as well. But, you know, it's very vulnerable to that type of abuse. The last thing I wanted to say was another potential vulnerability this time of year, people are getting ready to send to the IRS all their tax forms. And certainly that not only gives your income, but it gives you Social Security number and a ton of information about you. And maybe that's something for the public to be aware of, maybe you have a recommendation to do those by certified mail or return receipt.

MR. GRUPE:

I think for a number of reasons you want to do it by certified mail. But, yeah, that's something I would certainly advocate doing.

LEG. SCHNEIDERMAN:

Right. So it doesn't disappear from your mailbox.

MR. GRUPE:

Electronic filing of you income taxes has become another way, but again, that perhaps presents other opportunities.

LEG. SCHNEIDERMAN:

Thank you.

CHAIRMAN ALDEN:

Legislator Lindsay.

LEG. LINDSAY:

I too would like to thank the Special Agent, police officers and my old friend Michelle for coming today. This is something that really interests me and should really interest everybody, because it's so popular today. I don't think anybody hasn't been touched by this type of fraud. Michelle, how much money does Citibank lose a year because of fraud?

MS. DI BENEDETTO:

I actually don't have a handle on what the exact amount of money is, but I can tell you, Bill, is that Citibank has taken a great •• taken this issue extremely seriously, has put up a lot of firewalls that prevent you from getting further and further into, you know, the computer system where you can get online and get information.

LEG. LINDSAY:

My point is it must be •• you know, you mentioned globally it could be \$8 billion in the very near future. By point is that eventually, we all pay for that. I mean, it might not go on your personal account, but if the institution suffers that kind of loss, they have to make it up somehow, whether it be through insurance, which raises rates or they have to raise their fees on something. But I don't think anybody •• we're not ultimately immune from that.

MS. DI BENEDETTO:

What the banking industry has done and what Citibank has done is to put in place various initiatives that help prevent or reduce as you •• as Peter was talking about, reduce the amount of losses that are sustained. I mean, I can give you an example one of our employees, her husband does a lot of work on the West Coast, he has his Master Card, same joint account, she is on the East Coast doing transactions. She got five phone calls one night saying, we don't understand why your account number is being used on both sides of the United States. So you will find that more and more, when you use your credit card continuously on the same day, you may find out that you're going to get a telephone call saying, was that really you. You may also get at the register, when you're trying to use card, again, oh, by the way, we'll take a second form of identification, because you have used your card too much. So, I mean, those are ways in which we have put in safety measures to ensure that we are doing everything humanly possible to protect the customer.

LEG. LINDSAY:

What you were just talking about, about phishing. I was just the subject of one of those phishing episodes. We received an e•mail in my office about I do business with the Washington Mutual Bank, have a couple of accounts with them, and the e•mail said that your accounts, there's been an attempt to steal your identify through your online banking, and would you please go on this website and answer these questions. This just happened two weeks ago. Well, my office is located in an office building where there is a Washington Mutual Bank. So I didn't go online, I walked down the hallway and saw the manager, he said, this isn't from us, this is phony, and we have had a tremendous amount of problems with this with a lot of costumers.

MS. DI BENEDETTO:

That's the time when you hit the delete button and just wipe the whole thing off.

LEG. LINDSAY:

But it looks very legitimate.

MS. DI BENEDETTO:

It does. It does. You are right.

LEG. LINDSAY:

And, you know, I thought it was pretty clever to tell you the truth, because when I first saw it I didn't really think •• the fact that we don't do any online banking raised my awareness that there's something wrong here, otherwise I would have just complied with them, you know.

MS. DI BENEDETTO:

What we have done, Bill, at Citibank is to put in place difference safeguards. But what we've also done, I am the Community Relations Director for Citibank of Long Island, and I also have supervisory responsibility for Queens. And what we have done is go out, and I had sent to Legislator Alden, and I thank you very much for inviting me here today, is put together a seminar series which highlights identity theft, it also highlights what to look for, how to avoid it, and you're right, a shredder is part of the answer, because what happens is, and I bet you if we were ask how many of us around this room today got invitations in the mail to apply for credit cards or whatever, it has a lot of information on it. Those are the kinds of things that we don't throw in the plastic bag, those are the kinds of things that need to go into the shredder as well.

And one of the other things that we talked before was on your credit cards, we also let the •• our audience know as we're doing these seminars, that you can get your credit report for free. You can get it from three different companies that the Agent mentioned for free once a year, once a year, and they can do that as well. But what we have done is go out into the community, and I open this up to anyone who would like us to do it, we go out into the community, we go very grassroots, and we do identity theft seminars. And the give•away, if you will, or the raffle prize is a shredder. And it has been going very, very well. And when I wrote to Legislator Alden, I offered to say that we would be delighted to do it. If anyone wants us to do it, we will be delighted to go out into the community where you designate us to go, and we will do an identity seminar. We go into what is identity theft, how you can prevent it, and what steps you need to do to make sure that you're always protecting yourself. A lot of it was outlined by your presentation.

LEG. COOPER:

What is your contact number?

MS. DI BENEDETTO:

516•867•8269. As I said, we also have these in our financial centers, and it talks to how to be aware and how to protect yourself online. So I'll leave some of these here.

LEG. LINDSAY:

You know, I just learned something about the free credit check once a year. You know, we all have newsletters. It might be a good blip to put in there, you know, because of the outbreak of identify theft, you should do this once a year.

MS. DI BENEDETTO:

You're right. Because actually can know exactly, you know, what you charged, who you have your accounts with. And we have all of these in our financial centers all across •• there's 800 of them across the country, and you'll these, protect yourself, be aware of online fraud. And it's a free service that the bank gives.

LEG. LINDSAY:

And not to leave the police officers out of this. This is a relatively new unit, the Identity Theft Unit?

MR. COWIE:

Correct. I'd thank you also for inviting us. I'd like to thank also Mr. Zwirn for thinking of us. With that said, we were just invited a couple of hours ago, so I'm not ready for a presentation, but what I'd like to do maybe is just give you a little, if I could, snapshot of what we're doing and what we plan to be doing with our Identity Theft Unit. I'd also like to go back to a couple of those questions that I'd like to touch on that came up. My name is John Cowie, I'm a Sergeant, and I'm in charge of the Computer Crimes Unit. The Computer Crimes Unit consists of six detectives. It was created a couple of years ago to address computer related and internet related crimes.

About a year ago last April, we added two detectives who are with me today, Jim Crayne and Tom Gabriele, to address just specifically and identity theft, and created the Identity Theft Unit within the Computer Crimes Section. Since that time, we've added another sergeant and two detectives with the anticipation of adding a couple more detectives in the near future. We were just overwhelmed with the amount of identity theft cases coming into the unit.

Just some quick numbers. For last year, from April to the end of last year, 1140 identity theft cases in Suffolk County. And so far this year, about 400 identity theft cases. Some of the issues that have come up with identity theft are jurisdictional issues. Just by the nature of the beast, you know, our obligation and priority obviously is Suffolk County residents.

We have victim in Suffolk County, we investigate that crime and find out that our suspect and bad guy lives across the country. What that's done, that's kinds of •• I don't want to us the word force, because it's not a bad thing, but it's taken down some of the barriers between law agencies. We deal a lot with the FBI, postal inspectors and agencies all around the country. We oftentimes will have a bad guy that lives in our area and a victim in another jurisdiction. The identity theft cases can be prosecuted in either jurisdiction. And that's a good thing. It's, you know, opened up those lines between agencies.

We do think that one the biggest things is to prevent identity theft, that's probably the best message out there. We're still learning as we go here, but I do think that Suffolk County is, our Police Department is ahead of many, if not most departments with where we're going. And we have done some community presentations, and we like to do a community presentations and get out there and tell people how they can best protect themselves. Just because of the volume coming in, we are playing a little bit of catch up, we haven't really promoted it, but we won't turn anyone down who calls us and asks us to get out into the community and do a presentation. And that's something that we're certainly looking to expand in the future.

If I can just go back and touch on a couple of questions. I think Legislator Nowick was asking about the e•mail phishing type thing, and I think also yourself, Mr. Lindsay, with the different types, the Washington Mutual one, that's a common one that's around telling you you've won some money. There's all different ways of doing it, and it's all considered phishing. The best think to do is delete it. Oftentimes you find on the bottom that, you know, you're getting some kind of spam junk, pornography is a big thing. And it's common that they'll tell you that you're getting this because of your previous interests, and if you want to be removed from this mailing list, click here. That's the worst thing you can do because all that does is verify a e•mail address, which may not be as valuable as getting the bank information, but it's valuable, because a valid e•mail is just one more that they can add to the list of millions and millions they sent out. I think the Agent talked about sending out like 5000 and getting three or four, and that's true. But when you're sending out millions, you get hundreds of thousands of victims. So the best thing we suggest on any of that junk is delete it. You know, you can have it •• you can forward it to the Police Department, but a lot of these things are being done from overseas, they're very difficult to investigate. So with the junk, instead of deleting it •• the best think probably is to delete it, not click on any links that say click here to be removed from the list.

The online purchasing that you talked about, that's here to stay. You know, it's a part of our everyday lives, online shopping. And the best thing you can do is protect yourself, you know,

checking your credit cards, check you bank statements. It's difficult, but try to know who you are dealing with. And there's a lot of small mom and pop operations that are legitimate, but a website that can be created that, you know, look like Washington Mutual's website that someone is running out of a basement. That's not to say it's not a legitimate company, but I think when you're dealing with the big ones, you know, they are legitimate. Can something happen? Yeah, it can. You can have you credit card number stolen and be used. It's, like I said, a part of lives, it's here to stay. We talk about that with the kids with the IMing and the chatting. We need to dealing with it, because it's here to stay.

The credit card numbers that Legislator Schneiderman talked about, when you go out to a restaurant, they have these little palm side readers, and they're palm•sized, it's the size of a Bic lighter that can be held in your hand, you see them in some of the gas stations also, these guys can just swipe your card into that, and they have your number, just like they can •• you know, somebody can get a receipt and get your number off of your receipt. The best thing here is to just be cautious. You know, try to watch, try to pay attention. If the guy walks away with your card, it's something to be concerned about, but it happens. You know, try to watch them, try to make sure when you get the receipt that both copies are there, and if your number is on it, you certainly keep your copy.

The vacant house issue that you talked about with stuff being delivered. We've seen this. We've had issues where UPS and Fed Ex are delivering packages, you know, nonstop to a vacant house or to different names at the same address. And I was a little bothered by it that why didn't they call? But, you know what? They're in business, and they're being paid to make a delivery there, and they're delivering this stuff. So the vacant house thing is one of the things we try to do in our community talks is to pay attention maybe if there's a vacant house or an elderly person next door getting some packages. Certain people working all day, and there's packages left on the stoop during the day. Well, that's a because a neighbor or somebody is watching the house, maybe the kid across the street is having stuff delivered to that house because he knows everybody works there, and he runs over and grabs it during the day.

Like I said •• with that said, I wasn't really prepared to bring you up to speed. That's a snapshot of what we're doing and where we're looking to go. The Computer Crimes Section of the Identity Theft Unit, we right now are ten detectives and two sergeants, and that's only going to get bigger. There's, you know, a tremendous need. It's something that we will be •• we have been addressing. Like I said, I think we are at the forefront and we'll continue to stay at the forefront and respond to the community.

CHAIRMAN ALDEN:

Thank you. Jim Spero had a question, then I think Legislator Nowick does.

MR. SPERO:

Just a comment. I've been receiving a lot of these phishing e•mails right here at work, and they're apparently getting through the IS filter into to our Legislative systems. So I've authorized Allen Fung to buy an additional SPAM filter just for the Legislative system to try to block these e•mails from coming in also. There's also an interesting segment, I think it was on 60 Minutes or one of the new shows, that another scam they're doing now is when you have a wireless laptop, they drive •• they drive around the neighborhoods and the wireless laptop sends out a signal good for several hundred feet, when they drive and they catch somebody that's online as they're driving by, they're able to pick up the information as they drive by. So that's something else to be aware of.

MR. COWIE:

There's a name for that, and it's war driving. And there are ways to prevent that also. You have a wireless router set up in your house, but you need to set up security on that. And that is an issue, we've come across that in Computer Crimes Unit, they, you know, it comes back to this house because this is where the IP address is, but it's the kid across the street with his wireless going into. And that's something when you set up a wireless network in your house you need to address.

LEG. LINDSAY:

Could I? Just one comment. I hope Legislator Nowick does not shop online, because our shopping centers need to stay in business.

LEG. SCHNEIDERMAN:

And we need sales tax revenues right here in Suffolk County.

LEG. LINDSAY:

Last year, I think my son was one of your first customers when you first formed the unit. His identity was stolen, he thinks, by the office cleaning people. And it just drove him crazy for the longest time. In that process, there were able •• I mean, your unit was new at the time he went to the Precinct to report it, they didn't know you existed yet. And, you know, through talking to some people, I found out that you did and got all the information. But the purchases that were made on his credit card were all delivered to same address in Brooklyn. Do you follow up on that?

MR. COWIE:

We do. Ironically, or not ironically a lot of our business goes back into Brooklyn and Queens. We make a lot of •• we do a lot of cases, a lot of search warrants and a lot of arrests out of Brooklyn and Queens, which actually, in a way is kind of good, because it is something that we can still do from Suffolk as compared to, you know, when it comes back to Virginia, we're going to have to pass it off. But we do find an awful lot going to Brooklyn and Queens. And we follow up on everything. If it's something out of our jurisdiction that needs to get passed along, we will pass it along. If it's something we can do within our jurisdiction or within a drivable reasonable

area, we'll follow up and make the arrests.

CHAIRMAN ALDEN:

Legislator Nowick.

LEG. NOWICK:

I was just think about one other thing when you were talking from Citibank. I think that the system of making these calls when there are many, many purchases on a credit card, one right after the other, I think the call to the credit card owner, if you will, is a very, very good idea. And maybe I would direct this also to Peter, although you can go on the internet every day or every other day and check your credit card status and who's charging and who's not, that's okay for you and I, but I can picture somebody like my mom or my dad who can't even work a cell phone going on the internet to check their credit card. So I don't know if there could be some type of a federal law, because it's banking, I guess, requiring these banks to maybe •• even if it's a recording that goes out. I will tell you that I've had my credit card company call me when my •• you'll like this, Bill •• when my 21 •• 22 year old is home from school and she uses my credit card, I get these calls regularly. So you don't have worry about the stores around here when Keri is home. But it is •• it is really a very good way of stopping this. And I know it takes some manpower, and I probably would take some ••

MS. DI BENEDETTO:

There's two things that they do. One, they make a telephone call, especially in the example I gave you, bi coastal, and you know, same account number, two different people, one in California, one in New York, they do that as well. And what they also do is to do a series of •• you'll find some information sometimes in your Visa statement, your Master Card statement, you bank statement, and some of those little monthly inserts are extremely good to read up on even as you've described, your parents that didn't use the internet. And the other thing is check them on a monthly basis. So then you're only •• as you so aptly put out Peter, they are only out thirty days.

LEG. NOWICK:

That's easy checking on a monthly basis, because you are getting credit cards statements, you expect them every month, you fear them every month. That's easy. But going on the internet •

- but the idea of calling when there's a lot of usage ••

MS. DI BENEDETTO:

They will call. And they have done that for the last, I would say, 18 months to two years. They will actually call when there's transactions that are unusual. And if you have used your card •• as your daughter might be charging, charging, charging, charging, at some point, they are going to say to her, oh, by the way, may we have identification. I mean, that's happened to me when I went holiday shopping in Macy's, as an example. I bought three or four different items, when I got to purchase another one, they said, oh, by the way, Ms. Di Benedetto, will you be kind enough to give us a second form of identification? And to me, that made me feel good, because I said, wow, they're safeguarding ••

MR. GRUPE:

If I could add one thing. The credit card companies are doing a very, very good job. I mean, the average person doesn't realize exactly what the security department at American Express does. I mean, they do have problems with but•out schemes, all right? Bust•out schemes are •• when we talk about Brooklyn, I think of Brooklyn, I think of bust•out schemes, because, you know, we have bad guys who we are looking for all over the country. In the New York area, where do they all end up? In Brooklyn. I don't mean to offend anyone from Brooklyn here, but there are certain addresses, there are certain phone numbers that raise red flags to law enforcement and raise red flags to the credit card companies. Credit card companies track and store any telephone numbers that are called from to the credit card companies and any check or bank account information that's used to make a payment to the credit card companies. And I

bring this to everybody's attention, because the examples with goods being delivered to an address in Brooklyn, let's say, all right, if goods are purchased with American Express and they're going to be delivered to, you know, 123 John Street in Brooklyn, 123 John Street has a history, a negative history with American Express. American Express right away will identify that address as a problem address. They've got a terrific link analysis, they call it, _I2 Link Analysis_ that combines addresses, phone numbers, names, so on and so forth. I mean, there is a lot going on there that the average person is not aware of. But you know what? It's not enough, it really isn't.

LEG. NOWICK:

Thank you.

CHAIRMAN ALDEN:

I want to thank all of you for coming down. Just to sum it up though. I think what our job might end up being is something like what Bill pointed out and Jon Cooper pointed out earlier, if we could identify an area in Suffolk County, like, for instance, Vytra and our health benefits, if they're putting our full Social Security card •• our Social Security Number on an identification card that makes it easier to be stolen, we should take actions to stop stuff like that. So I think that, and I'm going to throw this out to Ben, if you want to use this committee as a conduit, you know, between the County Executive and the Legislature, we can develop a couple of areas like that where we can, you know, make an initial impact.

But also I think that we have to develop some kind of information, and whether we put it on our website or whether we make an information package available to the people of Suffolk County that Michelle Di Benedetto will come out from Citibank and do a presentation, you know, the FBI, Pete will come out and do, you know, a demonstration of, you know, like, what do that, what not to do. Suffolk County Police have a unit that's devoted to that. Make the people aware of some of the assets that we have in place, because I think right now there's you know, like, we have the access, we just, you know, don't have the information going out to the people. So whether we put it on the website and do it, you know, like maybe design something, whether we do it by resolution or do it. These are the steps you can take, and if you need more information, here's

the contact people that you can go to, and they'll make a presentation to your group, or you know, like, homeowner's association or whether it be senior citizens or whatever. And I think so we need to get the word out.

But now, I think we've also got, you know, like, some more resources that we could tap into. If you see something happening and you think that, you know, like, Suffolk County can make a difference by enacting some kind of legislation, you know, we've got a dialog now going. If you guys see stuff that's happening and you need our help, you know, as far as if we change the law a little bit it will help you out, you know, in certain aspects. The FBI, unfortunately, you know, we can't help you out too much, you've got to go to the federal guys, maybe Bush or whoever, but •• to make an impact, but if you can see something that we're doing that, you know, like, we can help ourselves out, you know, now we have a dialog open, and you can just keep us up on things like that.

Periodically I'd like to just revisit this. I'm going to contact Ben, you know, like, sometime later, maybe next week or something like that and see if we can set up a little bit of a format and develop a couple of those types of ideas. I think it would be beneficial to the people of Suffolk County. So I really want to thank you, all of you, for coming down and thank Ben for catching my miss on it great and getting you guys down, which was great. Thank you.

LEG. LINDSAY:

Any of those •• I'd like to involved in that if any ••

CHAIRMAN ALDEN:

I'd like to do it through the committee.

LEG. LINDSAY:

Yeah. That's fine. But I have some ideas I think that •• because I really think it needs to be done. Before they leave, I just want to mention about Michelle. Michelle is very active in the banking community for years, but like many of the people in our business community give of themselves freely, Michelle and myself served on the Board of the Long Island Housing

Partnership for many, many years. I know she has devoted an awful lot of time to the affordable housing issue on Long Island. She is a good person, and I thank her.

CHAIRMAN ALDEN:

That's where I first met Michelle, I was the attorney for the Town of Islip Community Development Agency, which we generate affordable housing. And Michelle •• her bank actually stepped up to the plate and did many, many projects, and they're still doing many projects. So I want to compliment you on that and thank you for ••

MS. DI BENEDETTO:

Thank you very much. I've been delighted to be here.

MR. GRUPE:

Thank you.

MR. COWIE:

Thank you.

CHAIRMAN ALDEN:

Thank you for coming down.

TABLED RESOLUTIONS

CHAIRMAN ALDEN:

We'll go to **IR 1037, (adopting Local law No •• 2005), a Local Law to require the installation of carbon monoxide detectors in connection with heating system conversions. (CARACCIOLO)**

Now, Charlie, I know wants to address us a little bit on that. So, Charlie, come on forward. Now, the sponsor of the bill told me that he had made some changes and that he had coordinated, and now, I hope, some of those things have ••

DIRECTOR GARDNER:

Yes. Mr. Chairman, I got the latest changes. And the Office and Legislator Caracciolo, we have had many discussions back and forth along with the Oil Heat Institute. I just didn't until a little while ago have the latest changes, I just got them. And there's only two, I think, two items that should be raised for discussion in the latest, And that is in the penalty section, which was changed, but changed at a time when we were discussing the requirements that were put on contractors. Since then, the wording has been changed to add homeowners to certain requirements, and I just raise the issue of that. This would be precedent setting in that this would be the first time that the Office of Consumer Affairs would be required to issues notices of violation and fines to consumers.

CHAIRMAN ALDEN:

Okay. And What's the second concern?

DIRECTOR GARDNER:

The second is that, and I spoke to Kevin Rooney just before he left, he does not know the numbers, and, you know, I always look at the impact on the office. So not to raise a roadblock to the law, but the point is we don't know the numbers involved, in other words, how many new heating systems are installed, because for each •• the way it is written now, for each new heating system, there would be two notices sent to my office. Now, that's 100, 200, big deal. If there's 300,000, that would be 600,000 pieces of mail. I don't •• the point is I have no idea what the number is. You know, we are a very small office, and I would hate to go ahead and say

yes and find out that we're going to get 150,000 pieces of mail coming into our office. I don't know what the numbers are and neither does Kevin.

CHAIRMAN ALDEN:

All right. With that being said, Bill Lindsay.

LEG. LINDSAY:

I got a problem with the consumer end of that, because how do we enforce that? I mean, if the onus is on the contractor, I mean, if you put out a spec to a contractor that on every conversion you do there has to be a, you know, detector involved, well, the contractor is going to enforce that, because he is going to sell you the detector and probably make money on it. You know, there's an incentive. But how do you do it with the homeowner, I mean, besides putting out a public notice, Charlie? I mean ••

DIRECTOR GARDNER:

Well, as far as the two forms, obviously, I can develop the forms. I would not •• the form that the consumer •• as this is written, the form that the consumer would be required to send to out office, I would simply make sure that the contractors have those. In fact, I spoke to Kevin, my idea would be to have one form that kind of incorporates both, in that the contractor would be signing the form developed by my office that would say, I have installed a new heating system on such and such a date at such and such a residence, and I have informed Ms. Jones, the homeowner, that she now needs •• she has 30 days to install a CO detector, signed by both, and then he could mail it back to me. So I •• because obviously, there isn't any way I could, after developing the forms, give all the forms out to consumers throughout the County.

LEG. LINDSAY:

I would rather see •• rather inform the consumer that the contractor install a hardwired detector

during the installation of the heating system and build it into the cost of the conversion.

CHAIRMAN ALDEN:

Well, the hardwire would require electricians too.

LEG. LINDSAY:

That's true.

CHAIRMAN ALDEN:

I'm not saying it's a negative, Bill.

DIRECTOR GARDNER:

Understand, as was mentioned before, CO detectors in order to be effective, need to be installed on any level where there are sleeping quarters, and that could be quite a distance away from the •• but that •• you know, whether it be contractors or consumers, the point is that I have a hammer with contractors in that they need a license. So if they don't do something, and any law, code, rule or regulation written by any town, county or state that licensed contractor does not live up to, they can be penalized by our office. It doesn't necessarily even have to be County code. So if the County said they have to do that, they would have to do it. I'm just raising the point that this law would authorize me to levy penalties on consumers, we've never done that before. I mean, you know.

LEG. LINDSAY:

How are you going to find them?

CHAIRMAN ALDEN:

Let me ask this question, and it's of Counsel. I had some discussions with Legislator Caracciolo, and I think he thought that he had actually deleted that, you know, making the penalty applicable to the homeowner, but if we, or if the Legislator that's the prime sponsor of this, if he

wants to make a couple of changes in this, can he do it if we discharge this without recommendation or does it have to go through another cycle anyway?

MS. KNAPP:

It would have to go through another cycle. The amended copy deadline was on Monday at five o'clock.

CHAIRMAN ALDEN:

So then the more •• I mean, the more prudent way to do it then would be to keep it in committee, let Legislator Caracciolo •• you know, if there was a mistake made, you know, maybe just a communication between him and I, then, you know, we can figure it out and then we can move it at the next cycle.

DIRECTOR GARDNER:

If I may. I just want to make sure that you understand that the wording in the penalties now, it was changed as a result of dialog between the office and Legislator Caracciolo. But it was changed after the first draft while we were still talking about just contractors. Since then, homeowners were added into mix and you know, now it just raises some concerns.

CHAIRMAN ALDEN:

I'm going to express that there was concern on all parts about the applicability of it to homeowner, and then the second part, at least •• there's three things. The second would be Legislator Lindsay's, you know, suggestion that it be hardwired, you know, that that's a little bit more enforceable.

DIRECTOR GARDNER:

And then the numbers. Again, even it's for •• I can develop forms, that's no problem. We can get forms out to licensed contractors, that's no problem. I just don't want to say yes to something that's going to generate a flood of, you know, hundreds and hundreds of thousands ••

CHAIRMAN ALDEN:

No. We're going to have to make a commitment to you that if we do this, you know, with those couple of little changes, like, number one, it can't apply to homeowners, but if we do this, and you do get flooded, we're going to have to take care of, you know, like, that problem for you, because we're creating that problem.

LEG. LINDSAY:

But not only that, but if •• I mean, we had in our spec for •• or is it the towns that require that the new homes have ••

DIRECTOR GARDNER:

State Building Code and Suffolk County Code, both, for new residences.

LEG. LINDSAY:

That's been in •• I mean, we had a big thing a couple of years ago with the electrical ••

DIRECTOR GARDNER:

New York State and Suffolk County both require that.

LEG. LINDSAY:

•• contractors weren't doing it or something, remember that, Charlie? We had to get after them.

DIRECTOR GARDNER:

Yes. Yes.

LEG. LINDSAY:

But my point is it's strictly the onus on the contractors, we license almost every one of these contractors now, so wouldn't it be a matter of you sending out a notice to all of your licensed contractors in this area either •• what would that be •• a modified electrical or plumbing.

DIRECTOR GARDNER:

Plumbing, most of them.

LEG. LINDSAY:

I mean, you have the data base of who to notify that would do the installations, right?

DIRECTOR GARDNER:

It's not a problem.

LEG. SCHNEIDERMAN:

It's a plug•in device, right? It's not a hardwired? So they would have to submit some form that said that they plugged it in into the hole, the wall socket, at this particular residence where they installed this system and then they would send you a copy of that.

DIRECTOR GARDNER:

The way it's written right now, it could be either type of device, correct. It doesn't specify that it has to be hardwired or not.

LEG. SCHNEIDERMAN:

Some towns, we talked about this earlier, do have permits, some don't, for changing the heating system.

DIRECTOR GARDNER:

Well, if you change to gas, you know, you need to have an inspection by LIPA or KeySpan or whatever they call themselves now. But a new oil •• if you go oil to oil, you don't necessarily need to have a permit for it.

LEG. SCHNEIDERMAN:

So how would your office be triggered? How would you ••

LEG. LINDSAY:

By the contractors that are licensed now.

LEG. SCHNEIDERMAN:

All right. So you could find out if ••

DIRECTOR GARDNER:

This would require the contractor who needs to be licensed to do this type of work, that contractor would then be, by this proposal, would be required to notify the Office of Consumer Affairs that on such and such a date at such and such a place they installed a new heating system.

LEG. SCHNEIDERMAN:

No. I like the idea of enforcing it through the contractor.

CHAIRMAN ALDEN:

Rather than the homeowners.

LEG. SCHNEIDERMAN:

Yes.

CHAIRMAN ALDEN:

Right.

LEG. SCHNEIDERMAN:

I'm just thinking, a lot of homeowners, should we pass this law, wouldn't even know that this law is in effect. I think really the onus should be on the contractor.

LEG. LINDSAY:

Not only that, when you're going for a conversion, you got to be going for 1000, 1200 bucks. The cost of a detector at that time, you know ••

LEG. SCHNEIDERMAN:

Just build it right into the cost of the system.

LEG. LINDSAY:

Yeah, and it's done.

CHAIRMAN ALDEN:

But as was pointed out earlier, you know, the cost of one like, you know, how can you quantify that?

LEG. LINDSAY:

Right.

CHAIRMAN ALDEN:

All right. So you are going to make a motion to table?

LEG. SCHNEIDERMAN:

Sure.

CHAIRMAN ALDEN:

I'll second that motion. All those in favor of tabling? All those opposed? 1037 stands **tabled**.

(VOTE:4•0•0•1)

(Not present: Legis. Cooper).

And I will contact the prime sponsor of the bill to see about those changes. Don't we have any questions for Cablevision about what's going on with the stadium and all that kind of stuff? No? All right. We stand adjourned then. Thanks a lot.

(* THE MEETING WAS ADJOURNED AT 2:34 P.M. *)

_ _ **DENOTES BEING SPELLED PHONETICALLY**